2009

Change Management Process

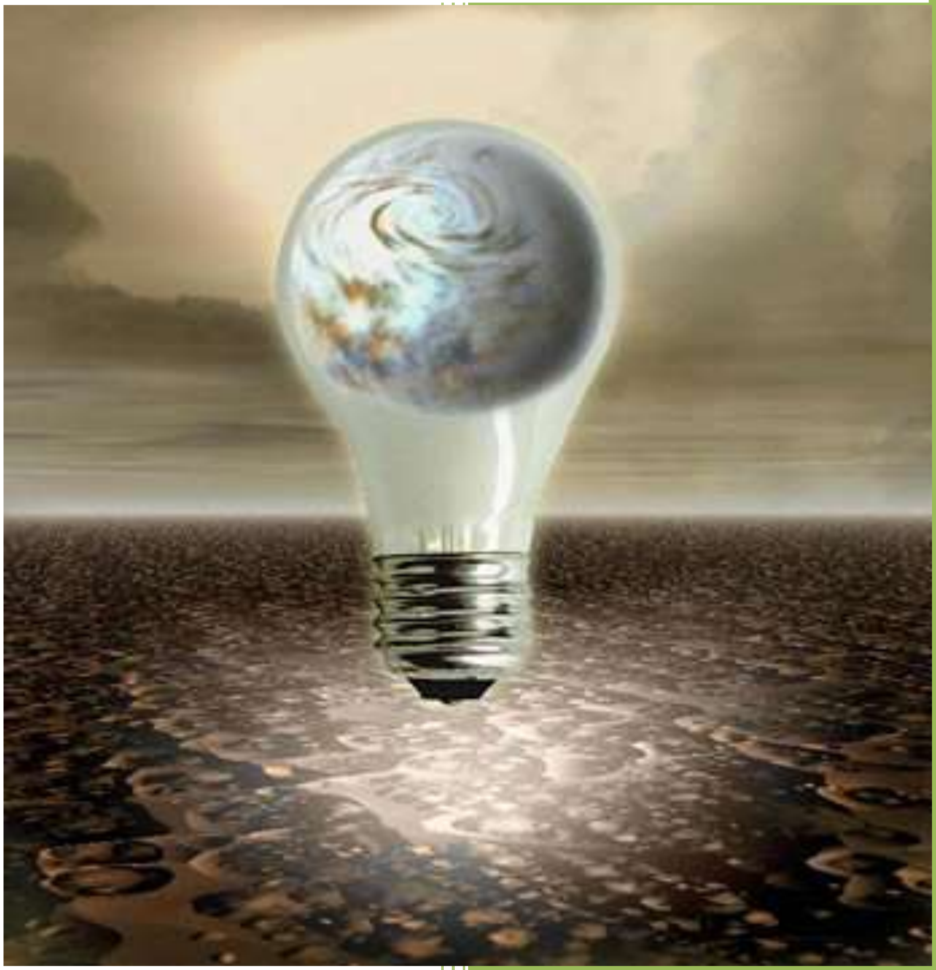


Table of Contents

CHANGE MANAGEMENT PROCESS

Purpose:

The Change Management process is to ensure standardized methods and procedures are used for efficient and prompt handling of all changes to minimize impact to the production environment.

Scope:

To establish a repeatable process, which can deliver efficiencies and effectiveness to protect the integrity of the King County production environment. To communicate and coordinate these changes to those affected, and preserve and publish a history of changes.

Participants in the Change Management Process:

Requestor

- Provide to the IT Manager\Supervisor\ITSDM the completed Request for Change Form.
- Assist the IT Manager\Supervisor\ITSDM to assess the level of Risk to implement the change.
- Participates in the Post-Implementation\Post-Incident Review

IT Manager\Supervisor\ITSDM

- Will review RFC for completeness, approve or deny Low Risk, no impact changes as they see appropriate.
- Responsible and accountable for all Low Risk, no impact changes within their section.
- Will acquire Division Director\ITSDM approval for Medium, minimal impact and High Risk, business impact changes.
- Will issue High Risk, business impact changes to the Change Advisory Board Chair for review and approval by the CAB Chair.

Division\Department Director\Designee

- Will review, approve or deny all Medium and High Risk Level changes for their Department.
- Responsible and accountable for all Medium Risk, minimal impact changes within their department.
- Will require all High Risk, business impact changes to be forwarded to the Change Advisory Board for review and approval by the CAB Chair.

The Change Advisory Board:

- Meet weekly on Mondays to review High Risk, business impact RFC’s.
  - Meetings will be cancelled if there are no High Risk RFC’s for review.
- Can request modifications to the change request..
- Make approval, modification or denial of change request recommendations to the CIO\Designee.
- Review Post-Implementation\Post-incident review of High Risk\ Business Impact and all Emergency changes.

The Change Advisory Board Chair

- Will facilitate CAB meetings
- Provide CAB recommendation to the CIO\Designee

The Change Coordinator – TBD

- Post meeting schedules, agendas, RFC’s, etc.
- Organize, schedule, and document the CAB meetings.
- Ensure the RFC forms are complete prior to placing them on the agenda.
- Record attendance and action items for each meeting.
- Maintain the SharePoint Website.
- Monitor centralized repository to track all change requests.
- Produce management reports for;
  - Current RFC’s issued and the status of each RFC.
  - Post-Implementation\Post-Incident Review for completion.
  - Historical RFC activity.
  - Change process metrics.
- Will inform Change Management Board Chair if an attendance problem exists.

Membership of CAB:

Change Advisory Board Chair	**Command Center**	**CAB Coordinator**
6 Month Rotation	**Cheryl Ann Gunderson**	**TBD**
Assistant CIO	**Public Health**	**DJA**
Roger Kirouac	**Lisa Hillman or Dale Hartman\Designee\SME**	**Carol Bertapelle \Designee or SME**
IT Operations	**DNRP**	**District Courts**
John Heath\Designee\SME	**Gary Hocking\Designee\SME**	**Cathy Grindle \Designee or SME**
Enterprise Services	**DOT**	**Assessor's Office**
Bob Neddo\Designee\SME	**Wayne Watanabe\Designee\SME**	**Hoang Nguyen \Designee or SME**
ADSS	**DDES**	**Office of Elections**
Ken Dutcher\Designee\SME	**Tom McBroom\Designee\SME**	**Laird Hail \Designee or SME**
CIS&PO	**DES**	**Prosecuting Attorney's Office**
Ralph Johnson\Designee\SME	**Katie Moriarty\Designee\SME**	**Fred Flickinger \Designee or SME**
OMB	**DAJD**	**Sheriff's Office**
Jim Walsh\Designee\SME	**Mike Holland\Designee\SME**	**Kelly Furner and/or Carol Gillespie \Designee or SME**
County Council	**DCHS**	**Superior Courts**
Paul Gaskill\Designee\SME	**Diep Nguyen\Designee\SME**	**Lea Ennis \Designee or SME**

CIO\Designee

- Primary – Roger Kirouac
- Secondary – Ayele Dagne

Benefits of Change Management:

- A repeatable process which can make changes in a timely manner
- Protects the integrity of a service or system when making changes
- Deliver process efficiencies and effectiveness
- Reduction of unauthorized changes
- Reduction in change related outages
- Reduction in emergency changes
- Coordination and communication of changes to minimize impact.
- Preserves history of changes.

Change Process Metrics:

The change process metrics will be used to encourage participation in the Change Management process, by giving positive recognition for the changes implemented through the change management process.

- Amount of time for CAB to process RFC
- % of successful changes
- % of failed changes
- % of Emergency changes

The following process is not intended to replace any department's current change management process they have in place. It is intended to be incorporated into existing change management processes, or to be used as a frame work for those agencies which do not have a change management process in place.

Change Management Process

STEP 1 (requestor)

Determine Type of Request for Change

EMERGENCY Change –Immediate change is required to avoid a complete failure, correct degradation of a service or to restore a system or service back to a normal state of operation. Such a change could not have been anticipated and therefore could not be scheduled. Emergency changes should be performed to restore services then an RFC and a Post Incident Analysis Form should be issued to the authorizing authority.
(Complete repairs then proceed to Step 6)

Final Notification to Customers: As Soon As Possible

STANDARD Change – are pre-authorized processes and procedures to implement a reoccurring change. These processes and procedures are well-known, well-documented and of low-risk for which authority has been given in advance. These processes and procedures are documented by the work group or best practices defined by the vendor. A standard change must be of Low Risk\No Impact to be considered as a Standard Change.
(Complete Steps 1-3 and 5-6)

Final Notification to Customers: One (1) Business Day, 24 Hours

NORMAL Change – The change is not of an emergent need and can be scheduled. There is not a pre-authorized process or procedure in place.
(Complete Steps 1-3 and 5-6, High Risk\Business impact will require step 4)

Final Notification to Customers:

Medium: Three (3) Calendar Days, 72 Hours
High: Five (5) Calendar Days, 120 Hours

Determine Risk Level

- Number of users impacted if an extended service outage occurred?
- Financial impact if an extended service outage occurred?
- The likelihood that a system/service failure could result in:
    - Disclosure of sensitive information which should be protected.
    - Misuse of client-owned resources
    - Malicious interruption of services
- Possibility of a system/service failure could impact safety, health, security, operational, or environmental.
- If this change implementation fails or adversely impacts other systems or services, what will be the impact of executing the rollback plan?

- Based upon past experience, what is the likelihood of failure or adverse problems resulting from the change?

Risk assessments are done by the technical staff implementing the change and their direct management. Risk assessments must take into consideration how much of the risk can you mitigate.

Determine Authorization Level

- **High Risk\Business** Impact changes need to be documented and processed through the Change Advisory Board. The authorization levels for these changes are by the CIO\Designee. These changes recorded in the change management database and post implementation reviews are done by the CAB.

- **Medium Risk\Minimal Impact** changes need to be documented and processed. The authorization levels for these changes are by the Division\Department Director\Designee. These changes are still recorded in the change management database and post implementation reviews are done by the Division\Department Director\Designee.

- **Low Risk\No Impact** changes will be determined by the IT Supervisor\Manager\ITSDM. These changes still need to be documented and processed but the authorization level is at the IT Supervisor\Manager\ITSDM level. These changes are still recorded in the change management database and post implementation reviews are done by the IT Supervisor\Manager\ITSDM.

Example: Signature Authority Requirements for Risk & Impact Levels:

Change Request		System or Service is….		
Change Risk & Impact Level	**Review and Approval Responsible\Accountable for change**	**Not Business Essential**	**Potentially Business Essential**	**Business Essential**
Low Risk\No Impact	**IT Supervisor\Manager\ITSDM**	🟩	🟩	🟨
Medium Risk\Minimal Impact	**Division\Department Director**	🟩	🟨	🟥
High Risk\Business Impact	**CIO\Designee**	🟨	🟥	🟥

Note: For Emergency Get Supervisor Approval, Then Implement

STEP 2 (requestor)

Complete the Request for Change Form

- **http://nocdocs/ChgMtg/default.aspx**
    - **On the left-hand side you will see a link for "Request for Change"**
- Select [New] fill out the form and select [Ok]
- An email will be sent to the Change Management Inbox

STEP 3 (manager)

Manager replies to requestors e-mail with Authorization Decision Authorization level

- If the RFC is of Low Risk\No Impact your IT Supervisor\Manager\ITSDM will authorize these changes.
- If the RFC is of Medium risk your IT Supervisor\Manager\or ITSDM will forward the RFC to your Division\Department Director\Designee for authorization.
- If the RFC is of High Risk the RFC will be forward to the Change Management mailbox for CAB recommendation and approval from the CIO\Designee.

Management Criteria for RFC Approval:

- Complete Implementation plan
- Complete Back out plan
- Complete Communication plan
- Complete Testing plan
- Valid Risk Assessment
- Have the customers and co-implementers been notified

Management Approval:

- Approved – RFC's classified as Approved are authorized to proceed as planned.
- Denied – RFC's classified as Denied are not authorized to proceed.
- Modification – RFC's classified as Modifications are requested to modify the RFC and return to the CAB for a Recommendation.

STEP 4 (Change Advisory Board)

CAB reviews RFC and makes a recommendation for authorization

- High risk\business impact changes go through the CAB
- Management Criteria for RFC Approval are the same
- Authorization Definitions are the same
- CAB will make a recommendation to the CIO\Designee
- CIO\Designee will issue Approval or Denial

STEP 5 (requestor)

Approved changes are implemented

STEP 6 (requestor, manager, and CAB for high risk RFC's)

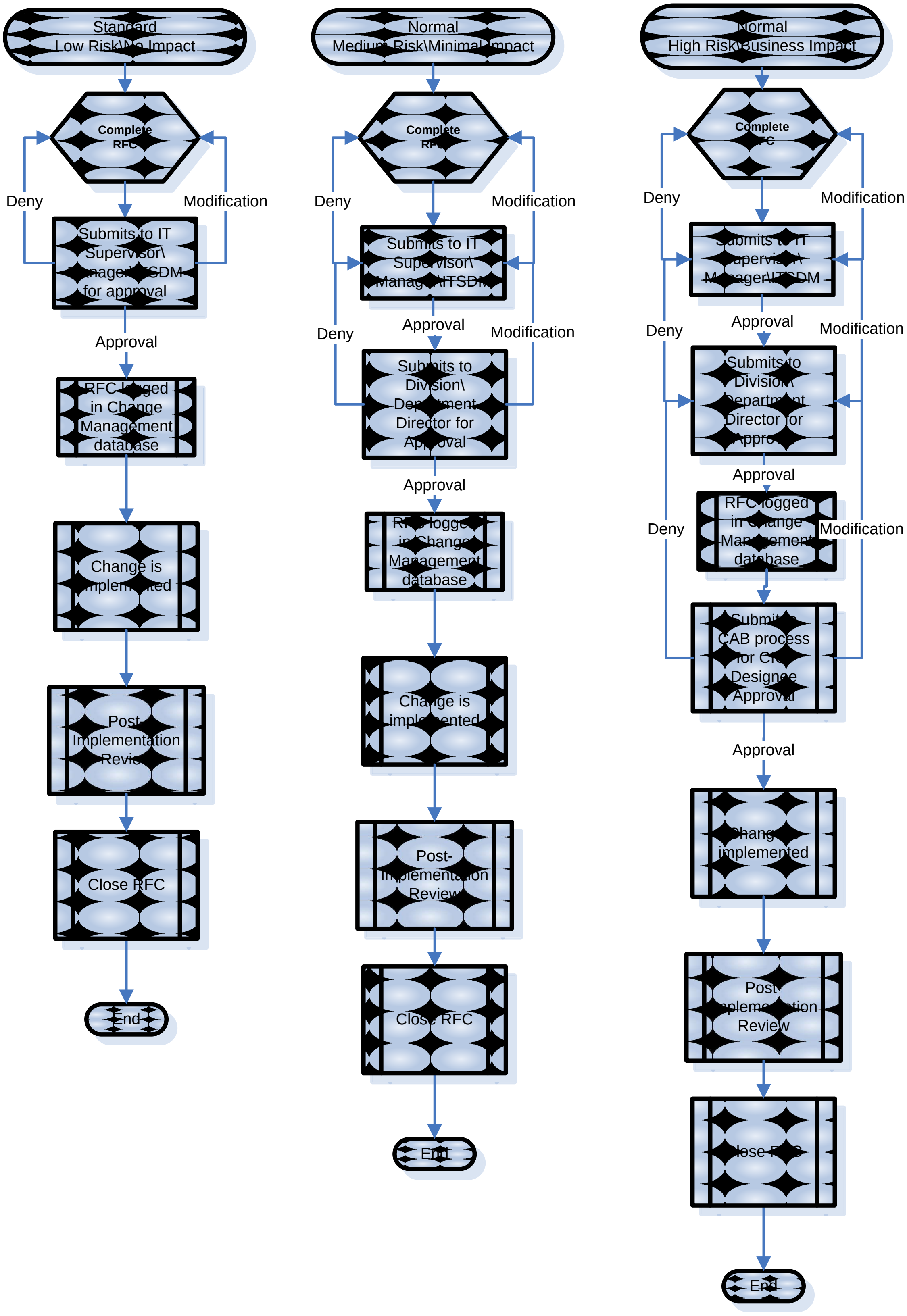
Post-Implementation\Post Incident Review:

Post implementation reviews should be completed at each authorizing level and documented within the RFC form and retain form for documentation.

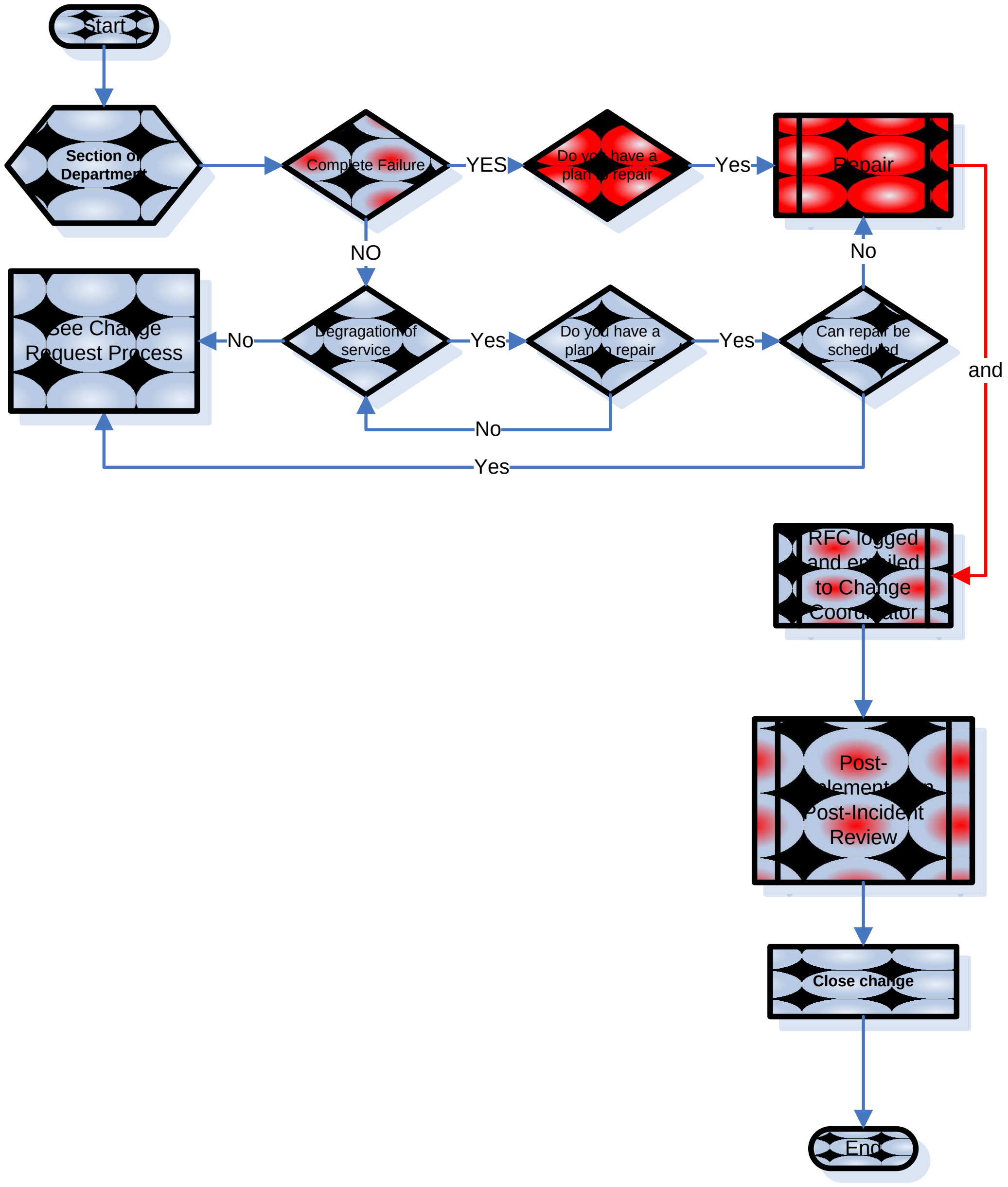
for:

- Successful Changes
  - Lessons learned
  - What went well
  - Closure of RFC
- Unsuccessful Changes – will also need a Post Incident Form
  - Lessons learned
  - What went well
  - What didn't go well
  - Cause of the post-change incident
  - Work a rounds
  - Completeness of change
  - Closure of RFC
- Post-Implementation\Post-Incident reviews not completed and presented to CAB will be escalated to senior management.

Change Request Process Flow


Standard
Low Risk\No Impact
Complete RFC
Deny
Modification
Submits to IT Supervisor\ Manager\ITSDM for approval
Approval
RFC logged in Change Management database
Change is implemented
Post Implementation Review
Close RFC
End
Normal
Medium Risk\Minimal Impact
Complete RFC
Deny
Modification
Submits to IT Supervisor\ Manager\ITSDM
Deny
Approval
Modification
Submits to Division\ Department Director for Approval
Approval
RFC logged in Change Management database
Change is implemented
Post-Implementation Review
Close RFC
End
Normal
High Risk\Business Impact
Complete RFC
Deny
Modification
Submits to IT Supervisor\ Manager\ITSDM
Deny
Approval
Modification
Submits to Division\ Department Director for Approval
Approval
Deny
RFC logged in Change Management database
Modification
Submit to CAB process for CIO Designee Approval
Approval
Change is implemented
Post-Implementation Review
Close RFC
End

Emergency Change Request Process Flow


Start
Section or Department
Complete Failure
YES
Do you have a plan to repair
Yes
Repair
NO
No
See Change Request Process
No
Degragation of service
Yes
Do you have a plan to repair
Yes
Can repair be scheduled
and
No
Yes
RFC logged and emailed to Change Coordinator
Post-Implementation Post-Incident Review
Close change
End

Quick Reference Guide

Change Management Steps				
Emergency	Standard	Normal	Steps	
🟪	🟧	🟩	1	A. Determine Type of Request for Change B. Determine Risk Level C. Determine RFC Approval Levels D. For Emergency get Supervisor Approval, then Implement
↓	🟧	🟩	2	A. Complete the Request for Change Form
	🟧	🟩	3	**Manager reply's to requestors e-mail with Authorization Decision** A. Authorization level B. Management Criteria for RFC Approval C. Management Approval:
	↓	🟩	4	**CAB reviews RFC and makes a recommendation for authorization** • Management Criteria for RFC Approval are the same • Authorization Definitions are the same • CAB will make a recommendation to the CIO\Designee • CIO\Designee will issue Approval or Denial
	🟧	🟩	5	**Implement Approved Changes**
🟪	🟧	🟩	6	**Post Implementation\Post-Incident Review Should be done by the implementation team and the signing authority**